AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

DIMITRIX JEROME KAY,

Defendant

Case No. 2:25-MJ-04307-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

As described in the accompanying attachment, defendant violated the following statutes:

Code Sections	*Offense Description*
18 U.S.C. §§ 1349 and 1028A	Conspiracy to commit wire and bank fraud, and aggravated identity theft

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s Lyndon Versoza
Complainant's signature

Postal Inspector Lyndon Versoza
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: July 14, 2025

Patricia Donahue
Judge's signature

City and state: Los Angeles, California

Patricia A. Donahue, U.S. Magistrate Judge
Printed name and title

AUSA Andrew Brown, 11th Floor, x0102

Complaint Attachment

Count One, 18 U.S.C. § 1349

Beginning in or before 2022, and continuing through the present, in Los Angeles County, within the Central District of California, and elsewhere, defendant DIMITRIX JEROME KAY and others conspired to commit wire and bank fraud, in violation of Title 18, United States Code, Sections 1343 and 1344. Defendant and his co-conspirators would steal the identities of victims to take over their financial accounts. Defendant and his co-conspirators would use the victims' identities and credit to obtain rental properties, credit cards, and other goods and services. Defendant would also falsely claim to be a relative of the recently deceased and ask their financial institutions to transfer the decedents' assets to defendant. Defendant and his co-conspirators used interstate wires to defraud their victims throughout this conspiracy. Federally-insured financial institutions defrauded by defendant include Wells Fargo Bank, US Bank, and JP Morgan Chase Bank.

Count Two, 18 U.S.C. § 1028A

Beginning in or before 2022, and continuing through the present, in Los Angeles County, within the Central District of California, and elsewhere, defendant DIMITRIX JEROME KAY knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person during and in relation to a felony violation of Title 18, United States Code, Section 1349, Conspiracy to Commit Wire and Bank Fraud, as charged in Count One, knowing that the means of identification belonged to another actual person.

AFFIDAVIT

I, Lyndon A. Versoza, being duly sworn, declare and state as follows:

I. SUMMARY AND PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of search warrants for the person and residence of DIMITRIX JEROME KAY for evidence of violations of 18 U.S.C. §§ 1028A, 1343, 1344, 1349, and 1956 and 21 U.S.C. § 844 (aggravated identity theft, conspiracy to commit wire and bank fraud, money laundering and possession of controlled substances (the "Subject Offenses")), as described in more detail in attachment B, which is incorporated by reference. The residence and person to be searched are listed below and described in more detail in attachments A, which are also incorporated by reference:

a. 13900 CHANDLER BLVD., SHERMAN OAKS, CALIFORNIA 91401 (the "KAY RESIDENCE") which is the residence of DIMITRIX JEROME KAY ("KAY"), and his mother Karisa Kay ("Karisa"); and

b. the person of DIMITRIX JEROME KAY.

2. This affidavit is also made in support of an arrest warrant and criminal complaint for DIMITRIX JEROME KAY for violations of 18 18 U.S.C. §§ 1349 and 1028A, conspiracy to commit bank and wire fraud, and aggravated identity theft.

A. Summary

3. DIMITRIX KAY is an identity thief with a long history of state violations related to identity theft. He is difficult to locate and often fails to appear in his court proceedings. Most recently KAY was apprehended by bounty hunters for bench warrants for failing to appear in his on-going state criminal proceedings.

4. On September 5, 2024, I, along with other law enforcement, executed a federal search warrant at 639 N Broadway, Apartment 526, Los Angeles, California 90012 (the "Tansuvit Residence"), which had been rented in the name of a victim of identity theft. Recovered in the residence were guns, drugs, and evidence of identity theft, such as stolen credit cards, fake Identity documents. KAY was present inside the residence during the execution of the warrant. I interviewed KAY who confessed to committing bank fraud and identity theft. He also told me he was on probation. Postal Inspector Emma Steele later searched KAY's phone and found messages showing his involvement in identity fraud. KAY's co-conspirators including Tansuvit, Hanson, Tinsley, Hailey Morris, and Frank Donan have been arrested and pleaded guilty for their roles in the fraud conspiracy. KAY continues to commit fraud against the estates of deceased persons, and resides at the KAY RESIDENCE with his

mother and together they both commit fraud.

II. TRAINING AND EXPERIENCE

5. I am a United States Postal Inspector employed by the United States Postal Inspection Service ("USPIS"), Los Angeles Division, in Los Angeles, California, where I have served since June 2005. I have been a federal law enforcement officer since 2002. Currently, I am assigned to the USPIS Contraband Interdiction and Investigations Team in Los Angeles, California, where I am designated as a Money Laundering Specialist. In this capacity, I am responsible for investigating criminal violations of money laundering and structuring laws, such as when the services of the United States Postal Service are employed by criminals as part of the means to launder or conceal illicit funds, and/or avoid financial reporting requirements. I am also one of seven Postal Inspectors in the U.S. currently designated by USPIS as a Subject Matter Expert ("SME") in money laundering investigations. As a SME, I have spoken at money laundering conferences and provided training to my colleagues, the financial and banking industry and other law enforcement agents. I have also received both formal and informal money laundering training from USPIS and other government and private agencies. Over the course of my career, my money laundering investigations

have led to the successful seizure of assets valued at hundreds of millions of dollars. During my approximately 20-year career as a Postal Inspector, I have investigated: thieves, burglars, rapists, mass-shooters, murderers, armed robbers, prison and street gangs, drug trafficking organizations, and perpetrators of financial violations (including money launderers, darknet vendors, digital currency launderers, identity thieves and fraudsters). For approximately five years, prior to investigating money laundering, I was assigned to investigate child exploitation and sex trafficking. In that assignment, I worked both independently and in a task force where I led and participated in investigations related to crimes involving the exploitation of children and sex trafficking domestically and internationally. In that capacity, I also earned a designation by USPIS as a SME in Child Exploitation Investigations.

6. From 2002 to 2005, prior to my service as a US Postal Inspector, I served as a law enforcement officer with the US Immigration and Naturalization Service, which later became part of the US Department of Homeland Security. In this capacity I enforced immigration and customs law at an international airport and seaport, and later, worked in an intelligence unit for local and national counterterrorism and human smuggling operations.

7. I am familiar with the facts and circumstances described herein. This affidavit is based upon my personal

involvement in this investigation, my training and experience, and information obtained from various law enforcement personnel and witnesses, including information that has been reported to me either directly or indirectly. This affidavit does not purport to set forth my complete knowledge or understanding of the facts related to this investigation. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and part only. All figures, times, and calculations set forth herein are approximate.

III. Statement of probable cause

8. The USPIS is investigating an identity theft and fentanyl trafficking crew run by Suppatra "Susie" Tansuvit ("Tansuvit"), Eric "E" William Hanson ("Hanson"), and James Bertrand Tinsley ("Tinsley"). Tansuvit, Hanson, and Tinsley regularly rented properties in the names of identity theft victims, mixed and sold fentanyl, and counterfeited identity documents. On February 21, 2024, the Los Angeles Police department executed a search warrant on a clandestine fentanyl laboratory located at 770 S. Grand Avenue, Unit 7069, Los Angeles, California. On June 5, 2024, the Los Angeles Police Department executed a search warrant on a second clandestine

fentanyl laboratory located at 2276 South Figueroa Ave, Los Angeles, California. As a result of these two search warrants, law enforcement seized approximately 15 kilograms of fentanyl, several firearms, and dozens of counterfeit identification cards. On September 3, 2024, the Honorable U.S. Magistrate Judge Stephanie Christensen authorized a search warrant for a third apartment located at 639 N Broadway, Apartment 526, Los Angeles, California 90012 (The "Tansuvit Residence"), which was executed on September 5, 2024. At the time of the search warrant's execution, DIMITRIX JEROME KAY was present at the residence.

B. DIMITRIX KAY Confessed to Conducting Account Takeovers of Deceased Individuals

9. On September 5, 2024, I conducted a voluntary interview of KAY where KAY agreed to talk to me. The interview was conducted inside a conference room within the United States Postal Inspection Service offices in Los Angeles. At the commencement of the interview, I offered KAY a beverage and an opportunity to use the restroom. I informed KAY that he was not under arrest, and that he was free to leave.

10. KAY provided the following information:

a. KAY stated he was on probation and has been on probation for over one year.

b. KAY stated he was introduced to Tansuvit because "I was doing fraud. And I'm not proud of it. I need to stop. My entire record's been fraud." KAY stated that his fraud was "just getting credit cards and stuff…from the deceased."

c. KAY said he uses the Los Angeles Medical Examiner website to search for deceased victims. KAY added:

> And I just cross my fingers and I go on Telegram and I just buy, literally, it's, it's too easy. They have these bots that are just instant, and it's like, you just type in the name and the zip code and bam, everything generates [and] populates within seconds. It's five bucks for the information. And I run a credit report and, you know, uh, I'll get the credit card and that's it. Just so I can get food and I take, you know, pay my bills. You know, I'm not trying to, you know, go crazy here.

d. KAY then said that he "has a knack for getting into online banking for Chase. I don't know why. It is just easy. And I would advise all of you now, if you bank with Chase, please… It's as simple as, um, it's, it's just absolutely pathetic how the security system is. All I need is the first and last name and the social security number and the birthdate and just basic common information, previous addresses and whatnot.

And I can call Chase, say, 'Hey, I forgot my username and password,' and literally bypass a few things. And then they read out to me over the phone letter by letter. I get logged in and, and you know… take over the account."

C. KAY Rents Vacation Homes to Defraud the Homeowners

11. In March 2025, a felon who claimed to have worked with KAY and hoped for leniency from the government ("CS-1") explained to me the following: KAY's modus operandi is to rent AirBNBs and gain access to the hosts' Wi-Fi and personal information. KAY would then use the Wi-Fi and personal information to open bank accounts and gain access to their existing bank accounts. KAY would then order credit cards to be sent to the hosts' address which he would intercept. KAY would also establish different phone numbers to help facilitate his fraud. He would then discard the phone lines and establish a new one. This is corroborated by a different individual who has worked with KAY, described next.

12. In May 2025, I interviewed one of KAY's co-conspirators who told me the following about KAY: He gets dead people's identities. He doesn't just use that identity, he becomes that person for months. When he is successful, he will rent luxurious hotels and Airbnbs.

D. DIMITRIX KAY's residence is associated with at least nine deceased individuals who did not live at the address

13. On February 14, 2025, I reviewed Credit Bureau databases and discovered that the 13900 Chandler Boulevard, Sherman Oaks, California 91401, which is where KAY resides with his mother when he is not at an Airbnb (the "KAY Residence"), was associated with at least nine deceased individuals, which is indicative of fraud. As outlined below, the credit report for each of the nine individuals showed activity at the KAY Residence that occurred *after* the date of their deaths:

e. Lariayn Payne

Date of death ("DOD"): March 5, 2024

Date of credit activity: September 10, 2024

f. Theodore Payne

DOD: January 11, 2024

Date of credit activity: September 10, 2024

g. Guy Langer

DOD: June 17, 2024

Date of credit activity: July 17, 2024

h. Albert Saltzmann

DOD: April 13, 2024

Date of credit activity: April 31, 2024

i. Elaine Osburn

DOD: June 11, 2024,

Date of credit activity: July 17, 2024

j. Julie McVie

DOD: April 25, 2024

Date of credit activity: June 30, 2024

k. Denise Foshay

DOD: December 15, 2022

Date of credit activity: December 29, 2023

l. Joshua Korczyk

DOD: August 22, 2017

Date of credit activity: May 26, 2022

m. Anthony Wolverton

DOD: January 14, 2020

Date of credit activity: March 5, 2022

14. I also reviewed evidence seized pursuant to the aforementioned search warrant executed on the Tansuvit Residence. One of the items seized was a Teachers Insurance and Annuity Association of America statement in the name of Lariayn Payne, one of the deceased victims identified above.

E. One of KAY's Current Phones is Associated with KAY and was used to Commit a $226,738.84 Fraud.

15. On June 6, 2025, I reviewed a report from the Teachers Insurance and Annuity Association ("TIAA"), which according to their website is a financial services company that specializes in providing retirement plans, insurance and investments for various trades.

16. According to TIAA, DIMITRIX KAY using the phone number (818) 214-9525 ("KAY Phone 1") conducted an account take over fraud on deceased victims Lariayn Payne, Ethel Edmonds Payne, and Theodore Payne. [for Kay's phones you have "Kay's Previous Phone

17. Beginning around March 2024, a suspect using a phone number 310 570 9170 accessed Theodore's TIAA account. On May 3, 2024, the suspect added the KAY Phone 1 and an email address I have seen KAY use previously (Iamthatgurrl@icloud.com), to the account. On June 5, 2024, a suspect contacted TIAA posing as victim Lariayn Payne and updated their address to 13900 CHANDLER BLVD, SHERMAN OAKS, CALIFORNIA 91401 (the KAY RESIDENCE). In July, a suspect using the name DIMITRIX JEROME KAY called TIAA and claimed to be the nephew/beneficiary of Lariayn Payne. On July 30, 2024, KAY requested and was sent three ACH withdrawals in the amounts of $134,137.41, $137,571.27 and $254,711.69.

TIAA initiated reversal of the withdrawals the next day. Only two of the reversals were successful leaving TIAA with a loss of $226,738.84.

F. KAY's Confession About Defrauding JPMC is Corroborated by Bank Reports.

18. On July 11, 2025, I reviewed banking reports and learned that, consistent with his admissions, where he said it was easy to defraud JP Morgan Chase accounts, I found numerous incidents of KAY committing fraud against that bank. For example, according to bank records:

a. Between March and June 2024, the names of DIMITRIX KAY, and his **mother Karisa Kay**, along with his co-defendant Hayley Morris were used in the fraud. A burner phone number was used to take over victim Theodore Payne's account. They then opened a fraudulent loan and credit cards and other activity that resulted in losses or attempted losses of $199,675.

b. In June 2024 KAY caused the fraudulent transfer of $191,448 from a victim at JPMC. On June 26, 2024, Alice Bonilla and KAY received $110,325. On June 27, 2024, three transfers totaling $81,123 were made to thebancorp.com Bank held in the name of KAY from the victim's JPMC account.

c. In June 2024, accounts held at JPMC in the name

of Donald and Marjorie Lievsay Revocable Family Trust were defrauded by KAY. On June 5, 2024, a Device Identification, a banking term for digital identification, was added to and given access to the Lievsay Trust accounts. Some of the funds from the accounts were then used make an unauthorized $100,513 ACH payment to Telsa for the benefit of KAY.

d. I found numerous other reports of similar conduct by KAY and his co-conspirators. Consistently, he would use the KAY RESIDENCE as the address for the account take over, but would also use other addresses like 888 S. Hope to direct some of the fraud. KAY appears to use different or multiple phone numbers for each victim. I counted about seven different phone numbers used by KAY in the three frauds listed in this section alone.

G. KAY Attempted to Steal $180,000 from the Estate of Victim Joel E. Rosner.

19. On May 30, 2025, I spoke with an employee ("CPG Employee") of Capital Pacific Group ("CPG"). According to CPG's website, "Our investigative team has been recovering assets on behalf of individuals, estates and corporations for Capital Pacific Group since 1991."

20. The CPG Employee told me they have been in correspondence with KAY since August 2024, where he told CPG

that he is the son of a deceased individual named Joel E. Rosner. KAY later signed a "Recovery Authorization Contract" with CPG, which authorized CPG to pursue unclaimed assets belonging to Joel E. Rosner's estate, including cash totaling over $49,000, and $101,875 in securities. According to the CPG Employee, KAY has been continuing correspondence with CPG with an email from KAY on May 29, 2025 where he said "Hey i finally got my birth certificate so i will be sending my documentation very soon."

21. Another CPG Employee also provided a saved voice message from KAY dated July 27, 2024. I listened to this voice message and immediately recognized the tone and cadence of the voice of the speaker as KAY. The message from KAY stated:

> Hi Timothy, this is Dimitri Kay. Um, I received a letter from your Capital Pacific Group Incorporated, uh, about Joel E. Rosner and the, um, basically the funds that need to be claimed. Um, I live at 1 3 9 0 0 Chandler Boulevard, Sherman Oaks, California 9 1 4 0 1 [the KAY RESIDENCE]. Um, Joel Rosner, unfortunately is deceased, so I don't know how I would go about claiming these funds, but if you could please call me back at (818) 214-9525 [KAY Phone 1] uh, and we could talk about it, um, it would help me out very much. Thank you again. That's 8 1 8 2 1 4 9 5 2 5 [KAY Phone 1].

22. On June 23, 2025, I spoke again with an employee of Capital Pacific Group.

23. The CPG Employee told me that on June 21, 2025, KAY sent a facsimile and email of a notarized "Claim for Forgotten Accounts" form in an attempt to support the claim that KAY is entitled to the estate of deceased victim Joel Rosen. KAY also provided a copy of his birth certificate and his identification card and social security card, all in his true name. I reviewed the claim form and saw KAY listed (747) 235 4554 ("KAY Phone 2") as his phone number.

24. In an email, the CPG Employee told me, "Attached is more information received from Dimitrix [KAY]. What he emailed/faxed in is not enough for the State to pay the claim. His birth certificate does not show Joel as his father."

25. I also listened to another saved voice message from KAY dated June 23, 2025. I recognized the tone and cadence of the voice of the speaker as KAY. The message from KAY stated:

> Hi, this is Dimitri Jerome Kay, uh, the claimant for the Joel E. Rosner, JP Morgan Securities, LLC refund. Uh, the account number is 1 0 0 2 4 7 6 1 3 7. Again, that's 1 0 0 2 4 7 6 1 3 7. I would like to confirm with you that I have faxed in the, uh, uh, form that you sent me to fill out and

get notarized. So I faxed that in along with, um, my id, my social security card and my birth certificate as asked. I also sent you an email of that fax, so please lemme know if you received it. If you please contact me at 3 1 0 7 0 6 8 7 4 8 ["KAY Phone 3"] as soon as you hear this, that'd be great. Again, that's 3 1 0 7 0 6 8 7 4 8 [Kay Phone 3]. Thank you. Bye-bye.

26. On July 3, 2025, the CPG Employee called KAY back at the KAY Phone 3. I listened to the conversation between KAY and the CPG Employee and a second CPG Employee after KAY got frustrated with the first employee. During this conversation, KAY asserted he was entitled to the unclaimed assets of Joel Rosen because he was the son of Rosen. When the CPG Employee pointed out that the birth certificate KAY provided listed "Norman Wayne Malone" as his father and not Joel Rosen, KAY stated that he did not know Norman Malone and that his promiscuous mother who was on drugs at the time was not sure who his father was. It was only later that a doctor declared through DNA that Joel Rosen was his actual father. Therefore KAY asserted that he was entitled to the unclaimed assets of Joel Rosen. When the CPG Employee stated a claim cannot be made unless KAY has proof that Rosen was his father, I then heard KAY consult with a woman on his side of the call (based on the context, it would have his mother, Karisa Kay). KAY and she

discussed if the medical clinic that did his paternity test still exists.

27. KAY explained during the call, "Right now bank, the claim, the claim form that, that Michelle sent me Yeah…was the JP Morgan Chase bank and the amount is a mature CD savings certificate and it was $479,000. I'm not trying to claim that one. I'm trying to claim the one that you guys sent me the packet for. You know what I mean? It is around $180,000 is his personal assets." The call ended with KAY stating he would file the claim directly with the state and not use CPG's services.

28. During the conversation KAY again stated his address was the KAY RESIDENCE.

29. The CPG employee told me that KAY had contacted CPG on at least four different phones. In my research, it appeared one of these phones may have been a Google Voice Phone number. In my training and experience, criminals who wish to avoid being found often employ many telephones, frequently dropping one line and adding another. By doing so rapidly, they can frustrate law enforcement attempts to locate them through their phone signal.

H. Dimitrix Kay and Coconspirators Exchanged Text Messages Containing Sensitive Victim Information and Tips for How to Fraudulently Take Over Accounts.

30. On September 5, 2024, KAY's previous cellular phone ("KAY's Previous Phone") was seized from the Tansuvit Residence pursuant to a search warrant signed by the Honorable U.S. Magistrate Judge Stephanie Christensen. Postal Inspector Emma Steele ("Inspector Steele") conducted a forensic review of the cellular phone, and told me she found the following:

a. On August 15, 2024 KAY's Previous Phone transmitted the following outgoing text messages to a phone number I recognized for Tansuvit at (747)-338-8480: "I was able to get 1000 out of the bank today" "I went to the same banker".

b. On August 16, 2024, KAY's Previous Phone received the following incoming text messages from a number I recognized as belonging to another co-defendant, Hailey Morris ("Morris") at (818) 928-9202: "Whatever happened to the USA credit card" "That never came?". In response, KAY's Previous Phone transmitted outgoing text messages, "It did" "Currently waiting for it to cool off if you know what I mean".

c. On August 16, 2024, KAY's Previous Phone received the following incoming text messages from Morris at (818) 928-9202: "Send me pic of id" "And give me the social".

d. On August 16, 2024, KAY's Previous Phone transmitted the following outgoing text messages to Morris at (818) 928 9202: "Please send me his sssn" "I fucjing reset my phone on accident". In response, KAY's Previous Phone received the incoming text message from Morris at (818) 928-9202: "I don't have it".

e. On August 16, 2024, KAY's Previous Phone received an incoming text message from Tansuvit at (747) 338-8480 which listed the name, date of birth, social security number, and fourteen addresses associated with victim Jon Yosuf.

f. On August 26, 2024, KAY's Previous Phone received the following incoming text message from Morris at (818) 928-9202, who texted KAY "As soon as I entered the card into and clicked submit this happened" followed by an image of a computer screen displaying the error message "Why have I been blocked? This website is using a security service to protect itself from online attacks. The action you just performed triggered the security solution. There are several actions that could trigger this block including submitting a certain word or phrase, a SQL command or malformed data." KAY's Previous Phone then received the following incoming text messages from Morris at (818) 928-

9202: "Aw shit" "Should I try again?" "Is the card still good for sure?"

g. On August 28, 2024, KAY's Previous Phone received the following incoming text message from Morris at (818) 928-9202: "If I get any phone line under the person's name will it work when I call Chase for the code." In response, KAY's Previous Phone responded: "Yes but u have to give it a few days when u update the number".

h. On August 29, 2024, KAY's Previous Phone received the following incoming text messages from Morris at (818) 928-9202: "Fuck man I'm sorry" "Well we know that's a good sign tho once we call I'm sure it'll get approved" "I expected this card to be locked and the card to not work" "That's my fault" "I'll fix it" "Tomorrow". In response, KAY's Previous Phone transmitted: "We should try to run the card on your square".

i. On August 29, 2024, KAY's Previous Phone transmitted the following outgoing text message to a number I recognized as belonging to Tinsley at (818) 582-7443: "Did you guys find the card?"

KAY Was Enlisted to Rent an Apartment in a False Name

j. On August 29, 2024, KAY's Previous Phone received the following incoming text messages from Morris at (818) 928-9202: "Hi my name is Josef I submitted an application and I got an email for id verification however when I try to log in the

website doesn't allow me to do so" "I need you to call encore apartment and talk to a leasing agent" "Say that".

k. On August 31, 2024, KAY's Previous Phone received an incoming text message from Tansuvit at (747) 338-8480 listing the name, date of birth, social security number, and fourteen addresses associated with victim Paula Weinstein.

l. On September 1, 2024, KAY's Previous Phone transmitted the following outgoing text messages to Morris at (818) 928-9202: "I knew my card could get fully unlocked I just needed to be in the right mindset" "And I did it my nigga" "I got that shit cleared". In response, KAY's Previous Phone received the following incoming text message from Morris at (818) 928-9202: "Ok let me know when it will go thru for the apartment".

m. On September 1, 2024, KAY's Previous Phone received the following incoming text messages from Morris at (818) 928-9202: "The documents have to be good and they want paystubs with. Bank statements" "They have to match" "On phone with bank". In response, KAY's Previous Phone transmitted the following outgoing text message: "Can we go jack yosufs mail".

KAY Had an Access Device Sent to Tansuvit's Apartment, Which Was Rented in the Name of a Victim of Identity Theft

n. On September 4, 2024, KAY's Previous Phone transmitted the following outgoing text message to Tansuvit

(747)-338-8480: "Did the Wells Fargo card arrive at the apartment".

o. On September 4, 2024, KAY's Previous Phone received the following incoming text messages from Tinsley at (818) 581-7443: "Nothing yet, I'll keep my eyes peeled." "What's the status of the tracking number currently?" The text messages were accompanied by a photograph of mail.

p. On September 5, 2024, KAY's Previous Phone received an incoming text message from (747) 225-6840 listing a name, date of birth, social security number, and eleven addresses associated with victim Jon Yosuf.

q. On September 5, 2024, KAY's Previous Phone transmitted the following outgoing text message to Tansuvit (747)-338-8480: "I got the PIN number for the us bank credit card tonight!!"

31. Based on my training and experience I know that members of a criminal conspiracy often communicate with one another to further the scheme. Commonly this is done by text, email, telephone, or specialty communication application. I believe that the above communications are referencing accounts that KAY and his co-conspirators were attempting to fraudulently access.

32. Also found in the phone were text messages between KAY and other co-conspirators trading images, front and back of

identification cards.

I. KAY has a long criminal history for Identity Theft is on Probation with the State of California with a Search Condition.

33. On June 4, 2025, I queried KAY's criminal history and observed he has been arrested for 12 felonies and has seven felony convictions, most of which were related to identity theft type crimes.

34. In May 2021, KAY was arrested by Burbank Police for CA PC 530.5(C)(2) (identity theft) and was sentenced in 2024 to two years formal probation. His records show that KAY's probation has been extended until April 2028.

35. I also learned that KAY was arrested in May 2025 by the Los Angeles Sheriff Department for his outstanding warrants. KAY bailed out in June 2025. (Shortly after his bail, KAY contacted CPG Employees to commit more fraud as described in the section above), while he was still on probation.

36. On June 4, 2025, I spoke with a LASD Detective about KAY's May 2025 arrest. The detective told me KAY was arrested by bounty hunters for his outstanding warrants. Bounty hunters are not law enforcement and did not provide any information to the sheriff's office of where KAY was arrested or if anything was found at the time of KAY's arrest.

37. On June 11, 2025, my analyst spoke with a LA County Probation Officer who confirmed that KAY was on probation and has frequently violated his probation. Probation said KAY resided at the KAY RESIDENCE. According to probation, KAY is to "*SUBMIT [HIS] PERSON AND PROPERTY TO SEARCH AND SEIZURE AT ANY TIME OF THE DAY OR NIGHT, BY ANY PROBATION OFFICER OR OTHER PEACE OFFICER, WITH OR WITHOUT A WARRANT, PROBABLE CAUSE OR REASONABLE SUSPICION.*"

38. According to KAY's most recent arrest by LASD, and his California DMV records, the location of his residence is at the KAY RESIDENCE.

39. KAY previously told me that he was addicted to methamphetamine. His criminal history is consistent with this statement. For example: In 2014, KAY was arrested for Possession of Narcotics. In 2015, KAY was convicted for Identity Theft, he was sentenced to probation and placed in a drug treatment program. In 2016, he was arrested for possession of a narcotics and theft. He was convicted for the fraud. In 2021, KAY was arrested for identity theft and possession of controlled substance and possession of controlled substance for sale.

40. On June 3, 2025, I conducted public records searches, using Thompson Reuters Clear database. Through these searches, I confirmed these record show that KAY resides at the KAY

RESIDENCE with his mother Karisa Kay.

41. On June 3, 2025, I queried USPS databases and observed that DIMITRIX JEROME KAY currently receives packages at the KAY RESIDENCE in his own name.

42. On June 6, 2025, I conducted surveillance at the KAY RESIDENCE where I observed a BMW X1 bearing the temporary license plate EB26X13 parked in the driveway. DMV Inquiries revealed this vehicle is registered to KAY's mother Karisa Kay.

KAY's Mother Karisa Kay Is a Drug Dealer Who Has Been to Prison

43. An inquiry of Karisa's criminal history shows numerous arrests and convictions. Karisa's first felony conviction in 1999 was for burglary. She had several arrests until 2011 when she was convicted and imprisoned for four years for burglary. In 2022 she was again convicted for burglary and sentenced to over 6 years imprisonment. In 2024, she was arrested for possession of control substance for sale.

44. On June 6, 2025, I spoke to LAPD Detective Justin Thomas. Detective Thomas said he had several investigations into KAY, Karisa and the KAY RESIDENCE. Detective Long said that Karisa is a drug user but also a known methamphetamine drug supplier.

45. In July 2025, I also spoke with the LAPD Senior Lead Officer who is designated as the community liaison for that

neighborhood. The officer told me that he had been to the KAY RESIDENCE multiple times, including for drug investigations. He said he had also been inside the residence in the past and found it to be a hoarder house, with dog feces scattered inside the house.

46. On July 11, 2025, I reviewed LAPD calls for service to the KAY RESIDENCE. From this review I found several calls in 2023, where the police noted incidence of violence also indicative of drug activity. For example:

a. On February 8, 2023, there was an aggravated assault with a weapon call to the residence. The notes stated that a 18th street gang member brandished a handgun at the residence;

b. On September 21, 2023, LAPD was called because KAY and another person named Penelope Zaranda struck Jackson Glenn Keith in the face with a closed fist and used a piece of wood to smash the windshield of a vehicle; and

c. On September 29, 2023, persons at the residence engaged in a argument that escalated and a person's phone was smashed in the street.

47. On July 11, 2025, I searched public records and found a report of a structure fire at the KAY RESIDENCE on May 13, 2025.

J. Training and Experience Regarding the Subject Offenses

48. From my training and experience investigating fraud, identity theft, and drug offenses, I know the following:

a. Members of criminal conspiracies must communicate with one another out of necessity. Commonly this is done by text, email, telephone, or specialty communication application, often an encrypted one such as WhatsApp, and most often by smartphone. Members of the conspiracy commonly carry their smartphones, which include the contact information for their co-conspirators, on or near their persons, such as in their cars or residences.

b. Individuals involved in identity theft and fraud schemes must keep evidence of their schemes, such as victim information and accounts used in the scheme, simply to keep the scheme going. Typically they keep these records where they have easy and private access to them, and where they feel the records are secure, most often their residence. Nowadays, much of this evidence is stored on digital devices such as computers and smartphones, which are also generally stored in the home.

c. Drug users typically have evidence of their drug use in their residences, such as controlled substances and related paraphernalia such as needles and pipes. They also

typically arrange their drug purchases through their smartphones, often by a secure messaging app arranging for a drug quantity, price, and delivery date and time. Typically the communication is opaque or somewhat coded, such as asking for "crystal" or "chrys" instead of methamphetamphamine, or "fet," or "confetti" for fentanyl.

d. Most criminals prefer to keep their criminal proceeds in cash so that their transactions are not traceable. More recently, some use cryptocurrency or peer-to-peer payment systems like Venmo or Zelle. Regardless of the payment method, professional criminals must keep track of payments to and from co-conspirators, as well as payments stolen from victims. Commonly this is done digitally. Many professional criminals will deposit some of their cash proceeds into bank accounts, or use them to purchase money orders or cryptocurrency, so that they can spend the proceeds at places that do not commonly accept cash payments, such as for rent, or store the proceeds safely.

K. Federally Insured Financial Institutions.

49. In my training and experience, all the financial institutions mentioned in this affidavit are federally insured. Also in my training and experience, it is all but impossible for persons to use smartphones and the internet without causing wire

communications to cross state lines. Internet communications are broken down into packets and sent by whichever route is most available at the time, which means that some of those packets are likely to cross state lines even if the sender and recipient are both in the same state. Further, major corporations, including telecommunications companies, generally maintain back-up data centers in different states to ensure that their data is not destroyed by a natural disaster, such as a wildfire, that might affect a data center in one state.

L. Training and Experience on Digital Devices.

50. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remains on the hard drive until it is overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary

directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading

filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

e. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

f. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

g. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an

average size of 1.5MB.

51. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress DIMITRIX JEROME KAY's and Karisa Kay's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of DIMITRIX JEROME KAY's and Karisa Kay's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

52. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

///

IV. CONCLUSION

53. For the above reasons, there is probable cause to believe that DIMITRIX JEROME KAY violated 18 U.S.C. §§ 1349 and 1028A (conspiracy to commit bank and wire fraud, aggravated identity theft), and that evidence, contraband, fruits, or instrumentalities of the Subject Offenses will be found at the KAY RESIDENCE and on KAY's person.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 14th day of July 2025.

Patricia Donahue

UNITED STATES MAGISTRATE JUDGE